Palantir's Tiberius, Race, and the Public Health Panopticon

The controversial data mining firm, whose history and rise has long been inextricably linked with the CIA and the national security state, will now use its software to identify and prioritize the same minority groups that it has long oppressed on behalf of the US military and US intelligence.

BY **JEREMY LOFFREDO** AND BY **WHITNEY WEBB** DECEMBER 7, 2020
31 MINUTE READ

English Español (Spanish)

Operation Warp Speed, the "public-private partnership" created to produce and allocate COVID-19 vaccines to the American populace, is set to begin rolling out a mass-vaccination campaign in the coming weeks. With the expected approval of its first vaccine candidate just days away, the allocation and distribution aspects of Operation Warp Speed deserve scrutiny, particularly given the critical role one of the most controversial companies in the country will play in that endeavor.

Palantir Technologies, the company founded by Alex Karp, Peter Thiel, and a handful of their associates, has courted controversy for its supporting role in the US military occupation of Iraq and Afghanistan as well as its participation in the detention of "illegal" immigrants through their contracts with the Department of Homeland Security and in "predictive policing" law enforcement programs that disproportionately affect minority neighborhoods. Equally controversial, but perhaps lesser known, is Palantir's long-standing and enduring ties to the CIA and intelligence community at large, which was intimately involved in the development of Palantir's products that now run on the databases of governments and corporations around the world.

The same national-security state that Palantir has long aided in oppressing countries abroad and minorities domestically is now running Operation Warp Speed. While Palantir's selection to manage the allocation of the vaccine to "priority groups" may just seem like the national-security state wanting to award the contract to a familiar and trusted company, the allocation strategy's heavy focus on vaccinating minorities first, with questionable justification for doing so, suggests something else may have been behind Palantir's selection to play a prominent role in Warp Speed.

Part 1 of this series on Operation Warp Speed and Race, "The Johns Hopkins, CDC Plan to Mask Medical Experimentation on Minorities as 'Racial Justice,'" explored Warp Speed's vaccine allocation plan in depth. That plan utilizes a phased approach aimed at "populations of focus" that had been identified in advance by various government organizations, including the CDC's Advisory Committee on Immunization Practices.

The main focus of this allocation strategy is to deliver vaccines first to racial minorities and in such a way as to make them feel "at ease" and not like "guinea pigs." This is particularly glaring given that these minorities will be receiving an experimental vaccine that allocation-strategy documents admit is likely to cause "certain adverse effects . . . more frequently in certain population subgroups," with research showing that those "subgroups" most at risk of experiencing adverse effects are these same racial minorities.

Part 1 also showed that the government believes information warfare and economic coercion will likely be necessary to combat "vaccine hesitancy" among these minority groups, rather than directly targeting the actual causes of this "hesitancy," namely, by addressing past instances of illegal medical experimentation on minorities by the US government.

This report, the second part of this trilogy covering the racist underpinnings of key aspects of Operation Warp Speed, reveals the real factors behind Palantir's rise to prominence as a national-security state contractor and the real reason why this company was chosen to identify the same "critical population" minority groups that it has been helping the US government oppress and surveil since the company's inception.

Tiberius Rising

On November 24, 2020, Secretary Alex Azar of the Department of Health and Human Services (HHS), a former Eli Lilly executive, announced that the department would begin conducting "practice runs" for Operation Warp Speed's distribution networks in anticipation of HHS's national roll out of a COVID-19 vaccine, which is set to begin in mid-December.

CNBC, reporting on Azar's comments, noted that Tiberius, a software program developed and managed by Palantir, "will help the federal government allocate the amount of vaccines each state will receive," and local officials will use Tiberius to "decide where every allocated dose will go—from local doctors' offices to large medical centers." According to that report and others, Tiberius would collect data from US government agencies, as well as from local and state governments, pharmaceutical firms, vaccine manufacturers, and companies like McKesson that have been contracted for the coming vaccine distribution.

Palantir's role in Operation Warp Speed was only announced in late October, with mainstream news outlets such as the *Wall Street Journal* reporting that the company was creating a new software product that would manage the production and allocation of COVID-19 vaccines in the operation's campaign. That mass of data will include "a wide range of demographic, employment and public health data sets" that will be used "to identify the location of priority populations" and make related decisions regarding the allocation of vaccine doses. Tiberius will also allow officials to "proactively identify distribution bottlenecks, inventory constraints, and gaps in administration across key populations."

AFP confirmed the *Wall Street Journal*'s reporting and noted that Tiberius would provide Palantir with access to sensitive health information so that it could "help identify high-priority populations at highest risk of infection." The Business Insider website noted that Tiberius would be capable of showing "areas with high proportions of healthcare workers, clinically vulnerable people . . . elderly people" or any other demographic deemed to be a "target population" by Operation Warp Speed. A separate report at Military.com quoted HHS's deputy chief of staff for policy, Paul Mango, as stating that delivery timetables and vaccine-delivery locations were "being mapped out" by Tiberius, which enables officials to see how many people in a given "target population" are in any US zip code.

Palantir's Tiberius uses the software that manages HHS Protect, a secretive database that hoards information related to the spread of COVID-19 gathered from "more than 225 data sets, including demographic statistics, community-based tests, and a wide range of state-provided data." HHS Protect has been criticized by several public health experts and epidemiologists, among others, because of the sudden decision by HHS to force US hospitals to provide all data on COVID-19 cases and patient information directly to HHS Protect. Hospitals have been threatened with the loss of Medicare or Medicaid funding if they decline to regularly feed all of their COVID-19 patient data and test results into the HHS Protect database.

HHS Protect, notably, contains protected health information, which several US senators warned in July raises "serious privacy concerns." According to a group of Democratic senators and representatives, "neither HHS nor Palantir has publicly detailed what it plans to do with this PHI [protected health information], or what privacy safeguards have been put in place, if any." They added that they were "concerned that, without any safeguards, data in HHS Protect could be used by other federal agencies in unexpected, unregulated, and potentially harmful ways, such as in the law and immigration enforcement context." Palantir is well-known for its controversial contract work with Immigration and Customs Enforcement (ICE), part of the Department of Homeland Security that uses Palantir software in immigration raids.

HHS Protect is also controversial for its newly added artificial intelligence–driven "predictive" component, which "uses prewritten algorithms to simulate behaviors and forecast possible outcomes." HHS has asserted that this AI component, called HHS Vision, was not built with software components purchased from Palantir, but with software from a smaller government contractor with close ties to IBM, another intelligence-linked tech giant.

In addition to the mass of information Palantir has access to through HHS Protect, the company is also a member of the COVID-19 Healthcare Coalition, a “collaborative private-industry response” involving Big Tech, NGOs, and health-care corporations that “share and leverage real-time data, best practices, and clinical expertise” for the official purpose of “preserving healthcare delivery” and “protecting people” during the coronavirus crisis. Other members, aside from Palantir, include Amazon, Microsoft, Google, Salesforce, and IBM as well as the CIA’s In-Q-Tel and the murky US intelligence contractor, the MITRE corporation. The massive amount of data shared by the coalition’s members, which also includes most major electronic health-record companies in the US, is aimed at “unlocking large-scale analytics for COVID-19.”

Tiberius, like HHS Protect, utilizes Palantir’s Gotham software, which has been “honed over a decade of partnership with military, civil, and intelligence communities,” according to Palantir’s product manager for Gotham, Ryan Beiermeister. In recent years, it has incorporated more aspects related to machine learning and artificial intelligence. According to *Forbes*, Gotham accumulates vast amounts of personal data that allow it to “map a person’s family members and business associates, as well as email addresses, phone numbers, current and previous addresses, bank accounts, social security numbers, and height, weight, and eye color.” It is usually favored by law enforcement and intelligence agencies and has been used (controversially) by several police departments, including in Los Angeles and New Orleans, as the cornerstone of “predictive policing” or precrime initiatives. A HHS spokeswoman stated that Tiberius will not use personally identifiable information.

Other reports have noted that Tiberius is involved to some extent in the clinical trials for COVID-19 vaccine candidates, which would also provide Tiberius with access to the data from those trials, including how various “population subgroups” react to a given vaccine candidate. As reported in Part 1 of this series, the Johns Hopkins guidance, on which the vaccine-allocation strategy was based, notes that it is likely that “certain adverse effects may occur more frequently in certain population subgroups.”

Those very subgroups with the greatest risk of experiencing adverse effects—ethnic minorities—are also the same subgroups set to be prioritized by the US government and identified by Tiberius to be vaccinated first during the official roll-out of Operation Warp Speed. Tellingly, those same ethnic minorities flagged by Johns Hopkins as priority groups are the same minorities that Palantir is best known for targeting through their controversial contracts with Department of Homeland Security’s Immigration and Customs Enforcement and law enforcement agencies.

Palantir and the Militarization of Health Care

New York Army National Guard Spc. Cody Roche records the total vehicle and personnel count that enter through the Entry Control Point of the Bronx-Lehman COVID-19 Testing Site on April 4, 2020. U.S. National Guard photo by 1st Lt. Kyle Kilner.

Tiberius is the most recent addition to—and perhaps the most emblematic—of Palantir's moves into the growing field of "public health" surveillance. In addition to Palantir's contracts related to HHS Protect, the company has also scored other COVID-19–related contracts with subdivisions of the HHS. As one example, it was Palantir that built the CDC web app for monitoring the spread of COVID-19, which has been actively collecting data since March 2020. The technology for this project was built on Palantir's Foundry software and "takes in a range of anonymized data from US hospitals and healthcare agencies, including lab test results, emergency department statuses, bed capacity and ventilator supply."

In early October, the National Institutes of Health Center for Advancing Translational Sciences awarded Palantir a $36 million contract for "enterprise data integration and data management," giving the NIH the Foundry-based public health software as well. In addition, according to federal procurement records, the US Coast Guard contracted with Palantir in April to help with its COVID-19 Readiness System. Palantir's contracting with the NIH preceded the COVID-19 crisis by a matter of months, with the company winning a NIH contract in January to provide "comprehensive data capabilities" for the President's Emergency Plan for AIDS Relief, according to *Forbes*.

Palantir is also gaining comparable data access to the UK population. In March, the UK's National Health Service awarded the company a $1.3 million contract to help develop its COVID-19 data store, with a similar mandate to help UK officials understand how to allocate resources appropriately. According to

CNBC, “the NHS health records, which Palantir has gained access to, includes patient names, ages, addresses, health conditions, treatments and medicines, allergies, tests, scans, X-ray results, whether a patient smokes or drinks, and hospital admission and discharge information.” More recently, the NHS has been in talks for a little over a month with Palantir to see about the company playing a role in “sensitive” contact tracing. Aside from the UK, Palantir has claimed to be involved in the COVID-19 response efforts of at least ten other governments in addition to the US and UK.

These lucrative public health contracts are set to be a long-term boon for the company, which recently went public. As InvestorPlace explained in late November, “the re-emergence of the pandemic this fall and winter in the US and Europe will lift Palantir’s revenue.”

Meanwhile, just as Palantir has been acquiring “contact tracing” contracts throughout the Western world during 2020, the company has also been dramatically expanding its contracting work with the US military, which has also been playing an outsized role in the COVID-19 response, especially with Operation Warp Speed. Though the military has contracted with Palantir for years, the company has recently acquired more contracts than ever with the Department of Defense, and it has recently supplanted long-favored defense contractors, like Raytheon, winning several key bids.

In February 2020, Palantir was awarded a massive $823 million contract with BAE Systems for the US Army’s Distributed Common Ground System, and a month later the company was awarded a $80 million contract with the US Navy to create and manage a new logistics system. Then, in April, Palantir won a contract with the newly created US Space Force to build “a common operating picture of space.” At the end of November, Palantir was awarded a contract of an undisclosed sum by the Army’s Futures Command, a command focused on Army modernization with a heavy emphasis on AI and machine learning.

Palantir’s increasingly successful acquisition of top military contracts began in earnest last year. In March 2019, Palantir won an $800 million contract to build the Army’s new AI-driven “battlefield intelligence system.” Then, in October 2019, Palantir scored a two-year $91 million contract to develop AI and machine learning capabilities for the US Army Research Laboratory. The deal includes both their Foundry and Gotham products, with Foundry spotting and flagging “risks” and Gotham integrating multiple data sets into one. By the end of last year, Palantir had scored yet another multimillion-dollar contract with the military for the Army’s Project Vantage. Also, in December 2019, it was revealed that Palantir had taken over the Pentagon’s AI drone-assassination program, known as Project Maven, which had proved too controversial even for Google, the company that had originally won the Maven contract.

While it may seem odd that Palantir would simultaneously win massive contracts from health-care agencies and the military, the military has, in fact, been heavily driving the takeover of US health care by the national-security state during 2020. Through partnerships with other leading Silicon Valley firms, the Pentagon is playing a major role in the COVID-19 response through Warp Speed, but it also is involved in other public health efforts that are technically unrelated, including predictive cancer diagnoses and “fitness” wearables. In addition, HHS—under the leadership of the HHS assistant secretary for preparedness and response, Robert Kadlec—dramatically deepened its partnerships with the Pentagon’s Defense Advanced Research Projects Agency (DARPA) over the same period. Palantir not only fits right in with this larger Pentagon-led initiative to militarize health care nationwide but the company is at its core.

A Tool of Surveillance and Oppression

As the previously cited reports have detailed, Operation Warp Speed is being almost completely managed by the US military, along with the Department of Homeland Security and the National Security Agency (NSA), as opposed to civilian health agencies, which, as noted in Part 1 of this series, are significantly less involved than in previous national-vaccination efforts and have even been barred from attending some Warp Speed meetings. The DHS, NSA, and the military all have multimillion-dollar contracts with Palantir.

In July, a government chart was obtained by STAT that showed "that roughly sixty military officials—including at least four generals—involved in the leadership of Operation Warp Speed have never worked in health care or vaccine development." One senior federal health official told STAT he was surprised by the number of soldiers in military uniform walking around the health department's headquarters in Washington, D.C. and said that recently he'd seen more than one hundred officials in the Warp Speed corridors wearing "Desert Storm fatigues."

Given Palantir's emerging role as the public health police, it's worth taking a step back to examine its record of enabling the racism and the militarism of US state violence. As noted by the *Guardian* earlier this year, "Palantir is well known in the defense and policing worlds."

Palantir has come under fire as a result of the company's contracts with Immigration and Customs Enforcement, including its creation an intelligence system used by ICE that is known as Investigative Case Management (ICM). The IB Times described ICM as "a vast 'ecosystem' of data to help immigration officials in identifying targets and creating cases against them" that also "provides ICE agents with access to databases managed by other federal agencies." ICM further gives ICE access to "targets' personal and sensitive information, such as background on schooling, employment, family relationships, phone records, immigration history, biometrics data, criminal records as well as home and work addresses."

This $92 million relationship between ICE and Palantir should cause concern, considering Palantir will be in charge of allocating "tailored" COVID-19 vaccines to the same minorities they're helping a militarized law enforcement agency target, "build cases against," and deport. In addition, as noted in Part 1 of this series, Warp Speed is set to explicitly prioritize both incarcerated individuals and undocumented immigrants of color, meaning that those incarcerated in ICE detention facilities, many of whom were placed there as a result of Palantir's other software, will also be flagged by Palantir's Tiberius software.

Palantir's work with ICE is hardly the sole reason controversies surround the company. It also has a close relationship with local law enforcement agencies and police departments across the country whom they supply with policing tools that overwhelmingly target minority groups. Some of those tools are "predictive," meaning that they flag individuals who have not committed a crime but, according to Palantir's data mining and algorithms, are "likely" to do so in the future. As noted by the *Guardian* in 2017, US law enforcement, in various parts of the country, have been using "Palantir to predict who will commit a crime by swooping Minority Report–style on suspects."

Police departments that have used Palantir's policing tools include but are not limited to the NYPD, LAPD, Chicago PD, Virginia State Police, and the New Orleans PD. Per its proponents, Palantir's policing tools harness the technology of big data to help police departments "streamline" law enforcement, thereby enhancing efficiency. Critics, however, say Palantir's tech creates "racist feedback loops" in which a "disproportionate amount of police resources are allocated to historically hyper-policed communities."

Notably, Palantir's predictive-policing methods were developed during the war in Iraq, a conflict where many legal red lines were crossed by the occupying forces. These aggressive policing techniques, forged during the fires of the so-called Global War on Terrorism, in which Iraqi citizens were almost completely denied their civil and human rights, are now being implemented in the US and elsewhere.

Palantir's law enforcement tools crunch data and identify certain areas of cities or neighborhoods that should receive an uptick in police presence. The Palantir police technology can create "chronic-offender bulletins," which attempt to predict and identify potential "repeat offenders" and problem areas.

After someone is deemed a possible or probable repeat offender, extra attention and enhanced surveillance techniques are deployed against that individual. Similarly, once an entire neighborhood is flagged by Palantir's algorithms as densely populated with repeat offenders, the neighborhood is considered a "hotspot zone" and is then more heavily policed, increasing the chance that residents will be stopped for minor infractions.

The Stop LAPD Spying Coalition criticizes the technological assumptions that underlie Palantir's algorithm-based policing as "pathologizing" individuals and entire neighborhoods. It says that the programs "enable the continuation of decades of discriminatory and racist policing under the apparent neutrality of objective data."

Palantir's policing tools also allow jurisdictions that normally would never communicate or share information to do so, resulting in a greater concentration of police power. As *Wired* noted, "When enough jurisdictions join Palantir's interconnected web of police departments, government agencies, and databases, the resulting data trove resembles a pay-to-access social network—a Facebook of crime that's both invisible and largely unaccountable to the citizens whose behavior it tracks."

Of all Palantir's predictive-policing efforts, arguably the most notorious took place in New Orleans. As revealed by The Verge in February 2018, Palantir had been secretly running a "predictive policing" pilot program for the New Orleans Police Department for six years and had been hiding it from the population of New Orleans and its city council. Key city council members were quoted as stating that they "had no idea that the city had any sort of relationship with Palantir, nor were they aware that Palantir used its program in New Orleans to market its services to another law enforcement agency for a multimillion-dollar contract." Two weeks later, the press office of the outgoing New Orleans mayor, Mitch Landrieu, told the *Times-Picayune* that his office would not renew its "pro bono contract" with Palantir.

As Palantir's role in "predictive policing" began to grow into a national controversy, another shady intelligence-linked company, Carbyne911—also funded by Peter Thiel— began contracting with police departments and emergency-service providers. Carbyne911, which received early investments from intelligence-linked figures such as Nicole Junkermann and the infamous Jeffrey Epstein, has stepped forward to take over what was once Palantir's predictive-policing portfolio for counties throughout the country. As explored in this article, Carbyne911 has a predictive-policing component that is eerily similar Palantir's.

In one recent example of Palantir-Carbyne baton passing, Carbyne911 entered into an agreement with the City of New Orleans this March, a deal that gave the company access to all emergency 911 call data and complete surveillance of those who call or interact with the city's emergency-services system, without any accountability or limitations. Just a month later, the New Orleans Police Department installed police checkpoints across the city.

Yet, Carbyne911's takeover of New Orleans in 2020 is not simply limited to 911 call-data collection. The company has also been involved in New Orleans official COVID-19 response from the very beginning. In March, Carbyne911 also claimed to be helping to "flatten the curve" in New Orleans.

Carbyne's recent pivot into public health followed the tarnishing of the company's public image over the past year, which was initially spurred by the Jeffrey Epstein scandal. After it was revealed that Epstein had invested a sizable sum in the company and that two of his close associates, Nicole Junkermann and former Israeli prime minister Ehud Barak, where Carbyne directors, the company became heavily scrutinized for its connections with Israeli intelligence.

Carbyne911 has since removed most of its original board of directors from public view in an effort to distance itself from Epstein-connected characters such as Junkermann and Barak and has also been using a company called Wowza to promote its services in an apparent effort to avoid further unwanted scrutiny.

Wowza Media Systems, which was founded in 2005 by David Stubenvoll and Charlie Good, partnered with Carbyne911 in 2015 to build what Wowza refer to as a "reliable, secure streaming ecosystem." In June 2020, the CEO of Wowza admitted that "New Orleans uses Carbyne's COVID-19 service to manage emergency calls and help individuals who have contracted the virus contact telehealth professionals instead of flooding emergency rooms. . . . Carbyne has been fielding 70 percent of the city's emergency calls, a majority of which were related to COVID-19 symptoms."

While the vast majority of Palantir's original predictive-policing programs have been discontinued over the past two years, its services are being replaced by Carbyne911. From New York to New Orleans, it seems that when one Thiel company relinquishes its control over public data, another Thiel-backed company emerges to take the reins.

The Mentality behind Palantir

Berlin, Germany, March 19, 2014. Hy! Summit – Image by Dan Taylor. www.heisenbergmedia.com

Aside from the company's role in aiding the US national-security state target minorities, it is also worth exploring the views on race espoused by Alex Karp, Palantir's CEO, and Peter Thiel, Palantir's cofounder, board member, and person most often associated with the company in the media. In late October, the *New York Times* published a lengthy profile of Palantir with a particular focus on its CEO, Alex Karp. In that article, Karp expressed his life-long obsessive fear of being murdered due to his "amorphous" racial background and that this fear "propels a lot of the decisions" that are made at Palantir.

New York Times writer Michael Steinberger described Karp's fear:

> "*"I still can't believe I haven't been shot and pushed out the window," Karp told me. We were in Palantir's New York office, located in the Meatpacking district. He wasn't being literal, despite the office's bulletproof windows and the bodyguards hovering nearby. Rather, he meant the feeling of inevitable doom that has plagued him since childhood. . . .*
>
> *He intuited from a young age that his background made him vulnerable, he said. "You're a racially amorphous, far-left Jewish kid who's also dyslexic—would you not come up with the idea that you're [expletive]?" Although he was now the head of a major corporation, neither time nor success had*

> *diminished the anxiety. If the far right came to power, he said, he would certainly be among its victims. "Who's the first person who is going to get hung? You make a list, and I will show you who they get first. It's me. There's not a box I don't check." His fear, he said, "propels a lot of the decisions for this company."*

A 2013 report published by *Forbes* noted that Karp has a 24/7 security detail that is explicitly there "to protect him from extremists."

It is certainly telling that Karp's longstanding and deep-seated fears of being targeted because of his ethnicity is a driving force behind many decisions that Palantir makes. Yet, while Karp professed to the *New York Times* that his fear is linked to a potential rise of "the far right," this claim becomes doubtful when examining the politics and views of Karp's close friend and Palantir cofounder, Peter Thiel.

A classmate of Thiel's at Stanford and now best-selling author, Julie Lythcott-Haims, wrote in 2016that Thiel had told her back when they were at university together that "apartheid was a sound economic system working efficiently, and moral issues were irrelevant." Lythcott-Haims went on to say that Thiel's statements gave her the impression that he was "indifferent to human suffering or felt that oppressing whole swaths of humans was a rational, justifiable element of a system of governance."

Though this is just one anecdote, Thiel's own subsequent statements and actions support this portrayal of his views. For instance, as the *New York Times* recently noted, "Thiel has argued that democracy and economic freedom are incompatible and suggested that giving women the vote had undermined the latter."

In regard to the claim about democracy and economic freedom, an August article from *Reason* on Thiel's political views provides more insight. For instance, Thiel wrote in 2009 that "I no longer believe that freedom and democracy are compatible," while a major ally of Thiel's, blogger Curtis Yarvin, claimed that same year that democracy was "a precancerous growth always pregnant with some malignancy."

Another influence on Thiel is German philosopher Carl Schmitt, a man infamous for his promotion of dictatorship as an inherently superior form of government. In a 2004 essay, Thiel used Schmitt's statement that "the high point of politics are the moments in which the enemy is, in concrete clarity, recognized as the enemy" in reference to the direction "the West" should take in the aftermath of September 11, 2001. At the time, Thiel had lamented that "a direct path forward" to face down the post-9/11 enemy "is prevented by America's constitutional machinery." It goes without saying that, at the time of the September 11 attacks, "the enemy" was perceived largely along ethnoreligious lines.

Thiel has also been linked to "white nationalists" and the "far right fringe," the very groups that fuel Karp's deepest fears, while individuals closely connected to Thiel, such as Jeff Giesea, are prominent supporters of "alt-right" personalities such as Mike Cernovich and Andrew "weev" Auernheimer.

Thiel's enduring close association with Palantir and his long-standing, close relationship with Karp discredits Karp's claim that his fear of being murdered for his ethnicity is solely based on fear of the "far right," given that Thiel is essentially the "far right" personified. Regardless of Karp's real reasons for feeling so afraid, what is clear is that race is at the forefront of his thinking and, thus, at the forefront of much of Palantir's company decisions.

Privatizing Total Information Awareness

In order to fully understand the incredible power Palantir wields and why it was chosen to serve such an integral role in launching Operation Warp Speed, it is important to understand who was really behind the rise of Palantir and why.

In general terms, Palantir was created to be the privatized panopticon of the national-security state, the newest rebranding of the big data approach of intelligence agencies to quash dissent and instill obedience in the population. This has long been a key objective of US intelligence, having been pioneered by the CIA as far back as the Vietnam War. It was covertly turned against the bulk of the US population by both US and Israel intelligence during the Iran-Contra and PROMIS software scandals of the 1980s, though efforts to use these big data approaches to target domestic protests and specific social movements had been ongoing for years.

The panopticon was originally an English philosopher's concept for a new, revolutionary prison design, but the idea was more fully developed by the French philosopher Michel Foucault. As independent journalist Johnny Vedmore reported in October, Foucault "would use the concept of Bentham's original Panopticon as a way to describe and explore 'disciplinary power.' . . . According to Foucault's work, disciplinary power had been successful due to its utilization of three technologies: hierarchical observation, normalizing judgment, and examinations."

Vedmore then notes:

> *Among the most notable of Foucault's analyses of the utility of the Panopticon is the following quote from his book Discipline and Punish: "The major effect of the panopticon is to induce in the inmate a state of consciousness and permanent visibility that assures the automatic functioning of power." In other words, the uncertainty of whether or not an individual is being constantly watched induces obedience in that individual, allowing only a few to control the many.*

It is perhaps unsurprising that for the recent profile on Palantir in the *New York Times* Karp chose to pose with three Palantir employees under a large portrait of Foucault.

During the Reagan administration, the individuals at the heart of the Iran-Contra scandal began to develop a database called Main Core, which firmly placed the US national-security state on its current, tech-fueled Foucauldian path. A senior government official with a high-ranking security clearance and service in five presidential administrations told *Radar* in 2008 that Main Core was "a database of Americans, who, often for the slightest and most trivial reason, are considered unfriendly, and who, in a time of panic might be incarcerated. The database can identify and locate perceived 'enemies of the state' almost instantaneously." It was expressly developed for use in "continuity of government" (COG) protocols by the key Iran-Contra figure Oliver North and was used to compile a list of US dissidents and "potential troublemakers" to be dealt with if the continuity of government protocol was ever invoked.

Main Core utilized PROMIS software, which was stolen from its owners at Inslaw Inc. by top Reagan and US intelligence officials as well as Israeli spymaster Rafi Eitan. Also intimately involved in the PROMIS scandal was media baron and Israeli "super spy" Robert Maxwell, the father of Ghislaine Maxwell and reportedly the man who brought the intelligence-linked child trafficker and pedophile Jeffrey Epstein into the Israeli intelligence fold. Like PROMIS, Main Core involved both US and Israeli intelligence and was a big data approach to the surveillance of perceived domestic dissidents.

The Iran-Contra and PROMIS scandals were exposed, but they were subsequently covered up, largely by the then and current US attorney general William Barr. Main Core persisted and continued to amass data. That data could not be fully tapped into and utilized by the intelligence community until after the events of September 11, 2001, which offered a golden opportunity for the use of such tools against the domestic US population, all under the guise of combating "terrorism." For example, in the immediate aftermath of 9/11 government officials reportedly saw Main Core being accessed by White House computers.

September 11 was also used as an excuse to remove information "firewalls" within the national-security state, expanding "information sharing" among agency databases and, by extension, also expanding the amount of data that could be accessed and analyzed by Main Core and its analogues. As Alan Wade, then serving as the CIA's chief information officer, pointed out soon after 9/11: "One of the post-September 11 themes is collaboration and information sharing. We're looking at tools that facilitate communication in ways that we don't have today."

In an attempt to build on these two post-9/11 objectives simultaneously, the US national-security state attempted to institute a "public-private" surveillance program so invasive that Congress defunded it just months after its creation due to concerns it would completely eliminate the right to privacy in the US. Called Total Information Awareness (TIA), the program sought to develop an "all-seeing" surveillance apparatus managed by the Pentagon's DARPA. The official agreement was that invasive surveillance of the entire US population was necessary to prevent terrorist attacks, bioterrorism events, and even naturally occurring disease outbreaks before they could take place.

The architect of TIA, and the man who led it during its relatively brief existence, was John Poindexter, best known for being Reagan's National Security Advisor during Iran-Contra and being convicted of five felonies in relation to that scandal. Poindexter, during the Iran-Contra hearings, had famously claimed that it was his duty to withhold information from Congress.

In regard to TIA, one of Poindexter's key allies was at the time the chief information officer of the CIA, Alan Wade. Wade met with Poindexter in relation to TIA numerous times and managed the participation of not just the CIA but all US intelligence agencies that had signed on to add their data as "nodes" to TIA and, in exchange, gained access to its tools.

Former Chief Information Officer of the CIA, Alan Wade as pictured on the Intelligence Issues website. www.intelligenceissues.com

The TIA program, despite the best efforts of Poindexter and his allies such as Wade, was eventually forced to shut down after considerable criticism and public outrage. For instance, the American Civil Liberties Union claimed that the surveillance effort would “kill privacy in America” because “every aspect of our lives would be catalogued,” while several mainstream media outlets warned that TIA was “fighting terror by terrifying US citizens.”

Though the program was defunded, it later emerged that TIA was never *actually* shut down, with its various programs having been covertly divided among the web of military and intelligence agencies that make up the US national-security state. While some of those TIA programs went underground, the core panopticon software that TIA had hoped to wield began to be developed by the very company now known as Palantir, with considerable help from the CIA and Alan Wade, as well as Poindexter.

At the time it was formally launched in February 2003, the TIA program was immediately controversial, leading it to change its name in May 2003 to Terrorism Information Awareness in an apparent attempt to sound less like an all-encompassing domestic surveillance system and more like a tool specifically aimed at “terrorists.” The TIA program was shuttered by the end of 2003.

The same month as the TIA name change and with a growing backlash against the program, Peter Thiel incorporated Palantir. Thiel, however, had begun creating the software behind Palantir months in advance, though he claims he can’t recall exactly when. Thiel, Karp, and other Palantir cofounders claimed for years that the company had been founded in 2004, despite the paperwork of Palantir’s incorporation by Thiel directly contradicting this claim.

Also, in 2003, apparently soon after Thiel formally created Palantir, arch neocon Richard Perle called Poindexter, saying that he wanted to introduce the architect of TIA to two Silicon Valley entrepreneurs, Peter Thiel and Alex Karp. According to a report in *New York Magazine*, Poindexter "was precisely the person" whom Thiel and Karp wanted to meet, mainly because "their new company was similar in ambition to what Poindexter had tried to create at the Pentagon," that is, TIA. During that meeting, Thiel and Karp sought "to pick the brain of the man now widely viewed as the godfather of modern surveillance."

Soon after Palantir's incorporation, though the exact timing and details of the investment remain hidden from the public, the CIA's In-Q-Tel became the company's first backer, aside from Thiel himself, giving it an estimated $2 million. In-Q-Tel's stake in Palantir would not be publicly reported until mid-2006.

The money was certainly useful. In addition, Alex Karp recently told the *New York Times* that "the real value of the In-Q-Tel investment was that it gave Palantir access to the CIA analysts who were its intended clients." A key figure in the making of In-Q-Tel investments during this period, including Palantir, was the CIA's chief information officer at the time, Alan Wade.

After the In-Q-Tel investment, the CIA would be Palantir's only client until 2008. During that period, Palantir's two top engineers—Aki Jain and Stephen Cohen—traveled to CIA headquarters at Langley, Virginia every two weeks. Jain recalls making at least two hundred trips to CIA headquarters between 2005 and 2009. During those regular visits, CIA analysts "would test [Palantir's software] out and offer feedback, and then Cohen and Jain would fly back to California to tweak it." As with In-Q-Tel's decision to invest in Palantir, the CIA's chief information officer at the time, Alan Wade, played a key role in many of these meetings and subsequently in the "tweaking" of Palantir's products.

It should come as no surprise, then, that there is an overlap between Palantir's products and the vision that Wade and Poindexter had held for the failed TIA program. One can see the obvious parallels between Palantir and TIA by examining how the masterminds behind each describe their key functions.

Take, for instance, the following excerpt from Shane Harris's book *The Watchers: The Rise of America's Surveillance State* regarding Wade's and Poindexter's views of TIA's "built-in privacy protections":

> *Wade liked the idea, but he heard something even more intriguing in Poindexter's pitch, a concept that he hadn't heard in any of the tech briefings he'd sat through since 9/11: the words "protect privacy." Wade thought that Poindexter's was the first ambitious information architecture that included privacy from the ground up.*
>
> *He described his privacy appliance concept, in which a physical device would set between the use and the data, shielding the names and other identifying information of the millions of innocent people in the noise. The TIA system would employ "selective revelation," Poindexter explained. The*

> *farther into the data a user wished to probe, the more outside authority he had to obtain.*

Compare TIA's "selective revelation" sales pitch with that recently offered by Karp and Thiel to the *New York Times* about Palantir's own supposed privacy safeguards:

> *Karp and Thiel say they had two overarching ambitions for Palantir early on. The first was to make software that could help keep the country safe from terrorism. The second was to prove that there was a technological solution to the challenge of balancing public safety and civil liberties—a "Hegelian" aspiration, as Karp puts it. Although political opposites, they both feared that personal privacy would be a casualty of the war on terrorism. . .*
>
> *To that end, Palantir's software was created with two primary security features: Users are able to access only information they are authorized to view, and the software generates an audit trail that, among other things, indicates if someone has tried to obtain material off-limits to them.*

The explanation offered by Poindexter and Wade for TIA and that presented by Karp and Thiel for Palantir are essentially analogous. Similarly, Palantir's "immutable log" concept, whereby "everything a user does in Palantir creates a trail that can be audited," was also a hallmark of the TIA system envisioned by Poindexter and Wade.

As noted in *The Watchers*:

> *Poindexter also proposed "an immutable audit trail," a master record of every analyst who had used the TIA system, what data they'd touched, what they'd done with it. The system would be trained to spot suspicious patterns of use. . . . Poindexter wanted to use TIA to watch the watchers. The CIA team [including Alan Wade] liked what they heard.*

The benefits in repurposing the "public-private" TIA into a completely private entity after TIA was publicly dismantled are obvious. For instance, given that Palantir is a private company as opposed to a government program, the way its software is used by its government and corporate clients benefits from "plausible deniability" and frees Palantir and its software from constraints that would be present if it engaged in a public project.

As this same late October *New York Times* profile on Palantir notes:

> *The data, which is stored in various cloud services or on clients' premises, is controlled by the customer, and Palantir says it does not police the use of its products. Nor are the privacy controls foolproof; it is up to the customers to decide who gets to see what and how vigilant they wish to be.*

From PROMIS to Palantir: Building the Public Health Panopticon

While Wade was involved in operating the information technology infrastructure of US intelligence and in guiding the rise of Palantir, he was also intimately involved in another company known as Chiliad. Chiliad was a data analytics company founded in the late 1990s by Paul McOwen, Christine Maxwell, and an unnamed third individual. However, *Bloomberg* lists Alan Wade as a cofounder of Chiliad, meaning that Wade, as the third cofounder, was involved in creating Chiliad while also serving in a top post at the CIA.

This is significant for two main reasons. First, Chiliad was developed into the very tool that became in demand by US intelligence in the immediate aftermath of September 11. It had been conveniently set up well in advance, however, allowing it to score key contracts thanks to the advanced stage of its product and its founders' intelligence connections. This, along with a glowing recommendation from the heavily compromised 9/11 Commission, benefited Chiliad's software, which was remarkably similar to early versions of Palantir and PROMIS software. Due to ongoing litigation in the PROMIS case, efforts were made by the US national-security state to retool and tweak the PROMIS software sufficiently so that it could argue that the software in use was dissimilar to the original stolen product, according to the original PROMIS developer, Bill Hamilton of Inslaw Inc.

Second, Wade, employed by the CIA at the time of founding Chiliad, created the company with Christine Maxwell, sister of Ghislaine Maxwell and daughter of Robert Maxwell. Before her father's death, Christine was intimately involved in and ended up leading the US-based front company that Robert Maxwell had used to sell versions of PROMIS, which had a backdoor to US national laboratories for Israeli intelligence, seriously compromising US national security. The CIA, alongside Israeli intelligence, was intimately involved in the PROMIS software scandal. Thus, the involvement of both Wade and

Maxwell in creating Chiliad and the clear overlap in the PROMIS and Chiliad software, suggests Chiliad was the US-Israeli successor to PROMIS. In addition, Wade's role in the rise of Palantir suggests that Palantir is yet another successor to PROMIS, a possibility also explored to some extent in this article.

Notably, Palantir began its rise to prominence as the go-to counterterrorism software of the West, just when Chiliad pivoted away from that sector, eventually folding a few years later. Notably, in the years prior to its shutdown, Chiliad had begun moving into health-care data, a pivot that became very obvious by 2012, when it began adding prominent health-care industry executives to its company board and getting involved in aiding "medical research."

Not long after Chiliad was shut down, Wade, who had also been the chairman of its board for many years, was added to the board of a UK cybersecurity firm called Darktrace. Darktrace, as noted in this article by Johnny Vedmore, is the result of the joining of UK intelligence with a team of AI researchers at Cambridge who were seeking to develop the AI "singularity." This attempt at "self-aware" AI was subsequently developed into "cybersecurity" software under the watchful eye and direction of UK intelligence. Darktrace's intelligence-linked software now runs not only a large swath of the UK power grid and the computers of major corporations around the world but also cybersecurity for the UK's NHS, giving it access to patient-health data.

Not long after Darktrace's foray into health care began, Palantir made its own pivot into health care, both for the NHS in the UK and HHS in the US. The latter partnership has expanded considerably over this past year, from HHS Protect to contact tracing and now to Operation Warp Speed. Meanwhile, Palantir's contracts with the US military, which is managing Operation Warp Speed, have also expanded considerably over the course of the past year. Palantir's expansion into nearly every sector of government is set to continue, particularly with president-elect Biden's pick to lead the US intelligence community—Avril Haines, who was a consultant to Palantir right up until she joined the Biden campaign as an adviser earlier this year.

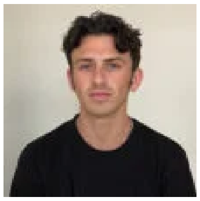
Like the planned all-seeing TIA apparatus, even mainstream outlets such as the *New York Times* have taken to describing Palantir as the "all-seeing eye," the center of a panopticon that has grown exponentially under the guise of a "private sector–led" response to a public health emergency. This "public health" panopticon, as clearly seen with Palantir and its role in Warp Speed, is all about advancing the long-standing goals of the national-security state and targeting the same populations targeted by state violence under the guise of "protecting" them and the collective. Palantir's objective is, and always has been, control of information and of knowledge and becoming the centerpiece of a vast surveillance enterprise that now extends far beyond the US borders.

The minority groups that Palantir has long targeted on behalf of the national-security state, and whom they will now identify and prioritize for Warp Speed vaccination, have long been the groups that the Western power structure has been most worried about rising up against the structural inequality and state violence that disproportionately affects them. It is thus no coincidence that the next leap of the surveillance state, through "pharmacovigiliance" and militarized aspects of Warp Speed, will target these same groups.

With military-led Operation Warp Speed and ICE-partnered Palantir gearing up to "tailor" certain COVID-19 vaccines to minority "target populations," we will next explore, in the third and final part of this series, the individuals surrounding one particular Operation Warp Speed vaccine. This vaccine has not only had a host of safety issues but was also developed by researchers with deep ties to the British Eugenics Society, which changed its name in 1989 to the Galton Institute.

Featured image: Palantir pavilion, World Economic Forum, Davos, Switzerland Photo by Cory Doctorow

AI cia COVID-19 Operation Warp Speed Palantir Surveillance



Author

Jeremy Loffredo

Jeremy Loffredo is a journalist and researcher based in Washington, DC. He is formerly a segment producer for RT AMERICA and is currently an investigative reporter for Children’s Health Defense.

Author

Whitney Webb

Whitney Webb has been a professional writer, researcher and journalist since 2016. She has written for several websites and, from 2017 to 2020, was a staff writer and senior investigative reporter for Mint Press News. She currently writes for The Last American Vagabond.

26 comments

BB says:
December 9, 2020 at 1:10 am

Keep up the fantastic work! “Skynet” came to mind when I read your artcile. It is hard to believe that so many people are naive and choose to be ignorant to the sinister plans behind “big government.” I am grateful to have your website to come to for real in depth analysis.
Reply

tony says:
December 9, 2020 at 4:28 pm

Thank you!!!
Reply

Jeff Carmack says:
December 10, 2020 at 8:52 am

If you watch Eric Weinstein's 2018 podcast with Thiel, then you will see how Thiel was covertly promoting the escalation of authoritarianism. Thiel's thesis: it is the utilitarian duty of governments to use violence against the people to speed up progress. Where do you think "warp speed" came from?
Reply

Jeff Carmack says:
December 10, 2020 at 9:05 am

*2019 podcast
The point is that Thiel and anyone with any power in intelligence knew the plandemic was coming.
Reply

Kelly says:
December 19, 2020 at 5:51 pm

https://historythings.com/historys-nutcases-tiberius/
Quite fitting name. Tiberius was a depraved Roman ruler and the adopted father of Caligula.
"Tiberius was a sick, sadistic emperor who had some disturbing torture methods. One of these involved getting his victims incredibly drunk, waiting for them to pass out and then sewing the ends of their penis shut. That was only the beginning of their torture. They couldn't urinate from that point on, which was something he used to his advantage as he tortured them further."
Reply

D says:
January 17, 2021 at 12:56 am

I was very surprised to see THREE Maxwell names here….Interesting.
Reply

Nemo says:
July 8, 2021 at 12:56 pm

Thiel is far right??? He's a socially left wing married homosexual man. He has systematically been given preferred leadership over various rightwing entities only to then water it down to libertarianism (which he professes, while having been originally uplifted by ex-communist neocon Irving Kristol, so he's really probably a socially libertarian necon, otherwise called a socially liberal Trotskyite). The Thai gentleman is an alt right guy? He's a gender fluid non white that was TROLLING. Mike Cernovich and Milo are bastions of the altright??? They're chaos agents intended to undermine the alt-right and reroute them to acceptable controlled pastures, which is hardly bad as Richard Spencer is a Russian agent, as I'm sure your Russian RT and Iranian

Mint Press intel agent overseers could confirm. Some of the info is good. A lot is disaaastrously bad. Two thumbs down. I’m disappointed in this agitprop. I recommend further training at the quds force camp.
Reply